Delivering Energy Networks Security: Economics, Regulation and Policy

Tooraj Jamasb[1], Durham University Business School, UK and Rabindra Nepal[2], School of Economics, University of Queensland, Australia

Introduction

In recent years, security of energy supplies has re-emerged as a major policy concern. At the same time, there is a growing concern with regards to the physical and cyber security of critical infrastructure of strategic importance such as telecommunications, water supplies, transport systems, and energy supplies. Physical and virtual networks serve as the nerve system of critical infrastructures and, while vital for the functioning of these facilities, due to their geographic spread, they are vulnerable to natural disasters and malicious threats. As the modern economy are increasingly dependent on reliable but increasingly complex network infrastructures, the vulnerability of these and the cost of potential failure also increase. This chapter focuses on the economics, regulation, and policy aspect of the security of energy networks.

Delivering Energy Network Security

Economics of network security

Energy networks are generally regarded as natural monopolies. This implies that the cost structure of these networks is such that their capital costs constitute a high portion of their total costs. This in turn results in declining average costs as the scale increases. As a result, it is more cost effective for a single network to serve the whole sector than by multiple competing firms. It then follows that, in the absence of competitive markets, these networks are, in the public interest, in public ownership or are subject to economic regulation.[3] In most European countries, prior to the 1990s, the energy networks were in public ownership and under oversight of the relevant ministries. In the USA, the major network utilities have traditionally been privately owned and regulated by Public Utility Commissions (PUCs) or the Federal Energy Regulatory Commission (FERC).

In economic terms, the decision problem with regards to provision of network security can be framed as the level of precaution required to minimize the total cost of the expected value of damage of security incidence. The expected value of damage can be viewed as a decreasing function of the product of probability of an incident occurring multiplied by the value of damage from the incident. This damage must then be weighed against the cost of undertaking precautionary efforts to prevent the incidence (as an increasing function of precaution). The economically point is then where the sum

[1] Tooraj Jamasb is Chair in Energy Economics at Durham University Business School and Co-Director of Durham Energy Institute. He can be contacted at Durham University Business School, Mill Hill Lane, Durham DH1 3LB, UK. Email: tooraj.jamasb@durham.ac.uk.

[2] Rabindra Nepal completed his PhD in Economics with a specialisation in Energy Economics as a James-Watt Scholar under the Scottish Graduate Program in Economics (SGPE). He has previously held appointments with Heriot-Watt University, UK and the University of Oklahoma, USA. He can be contacted at r.nepal@uq.edu.au.

[3] Armstrong, M., Cowan, S., and Vickers, S.J. (1994), '*Regulatory Reform: Economic Analysis and British Experience'*, Cambridge, Mass: MIT Press.

of total costs of expected damage and those of precautionary efforts are minimised. It is, however, possible to deviate from this minimum efficient cost level for security, social, or other considerations.

Incentive regulation for network security

Since the 1990s, the economic regulation regimes in many countries have gradually shifted from cost-based regulation to incentive-based regulation models. Cost-based regulation covers the costs of a network utility plus a set rate of return. However, the incentive properties of this approach can in theory and in practice result in cost inefficiency and over-investments.[4] Consequently, some sector regulators have adopted incentive based regulation models that reward input cost efficiency or quantity and quality of outputs.

The theoretical and methodological advances in recent decades have enabled the sector regulators to adopt innovative incentive-based models for economic regulation of network utilities. Incentive regulation can be facilitated by the use of efficiency and productivity analysis techniques for benchmarking of network utilities and to reward or penalise cost and quality of service efficiency performance.[5] In the absence of market mechanisms in the network sector, benchmarking is used to mimic a competitive market situation and to reduce information asymmetry between the sector regulators and the regulated firms.[6]

The existing incentive-based regulation and utility benchmarking models can be adapted and modified to address energy networks security concerns.[7] Within this approach, network security can be conveniently viewed as an extension of performance standards and economic regulation of quality of network services.[8] Incentive regulation of network security can then either focus on network security inputs i.e. capital and operating costs and network security outputs or performance measures such as the number and frequency of long interruptions. This general framework can be used in both input-based and output-based regulation.[9]

The policy makers and sector regulators have a few options in disposition. They can treat the security costs as a pass through item – i.e. the utility can invest an agreed upon amount on security and recover these through its network charges. Alternatively, the regulation can treat the security costs as investment and allow the utility to earn a rate of return on these. Another option is that the regulator can subject the costs of security

---

[4] Averch, H. and Johnson, L. (1962), 'Behavior of the Firm under Regulatory Constraint', *American Economic Review*, 52(5), 1052-1069.

[5] Giannakis, D., Jamasb, T., and Pollitt, M. (2005), 'Benchmarking and Incentive Regulation of Quality of Service: An Application to the UK Electricity Distribution Networks', *Energy Policy*, 33(17), November, 2256-2271.

[6] See: Shleifer, A. (1985), 'A Theory of Yardstick Competition', *The RAND Journal of Economics*, 16(3)(Autumn), 319-327; Jamasb, T. and Pollitt, M. (2001), 'Benchmarking and Regulation: International Electricity Experience, Utilities Policy', 9(3), 107-130.

[7] Jamasb, T. and Nepal, R. (2015), Issues and Options in the Economic Regulation of European Network Security, *Competition and Regulation in Network Industries*, 16(1), 2-22.

[8] Jamasb, T., Orea, L., and Pollitt, M.G. (2012), 'Estimating Marginal Cost of Quality Improvements: The Case of the UK Electricity Distribution Companies', *Energy Economics*, 34(5), September, 1498-1506.

[9] Cambini C., Croce A., Fumagalli E. (2014), 'Output-Based Incentive Regulation in Electricity Distribution: Evidence from Italy', *Energy Economics*, 45, 205-216.

improvement to incentive regulation - i.e. to offer economic incentives to achieve a desired security level. This can be done by including a new component Q^* to the conventional price/revenue cap incentive model as in Equation (1). Q^* is network security adjustment factor that reflects continuity of supply, for example, in terms of long unplanned supply interruptions. The allowed price (or revenue) path P_t of the company is then directly linked to network security performance where; X is the efficiency improvement factor obtained from cost and service quality efficiency benchmarking, and RPI is the retail price index.[10]

$$P_t = P_{t-1}\,(1 + RPI - X + Q^*) \qquad (1)$$

Within the above approach, network security can be conveniently treated as an extension or aspect of quality of service. This is possible because quality of network services is already subject to regulation in most countries as an incentivised output or through mandatory performance standards.

Network security policy

In addition to the economic regulation approach, policy makers have another option to consider. They can view security of the network infrastructure as a strategic priority for national security. This view suggests that the security costs can be covered from the national security budget. This approach entails that security costs can be imposed on network utilities and paid for by the taxpayer (as opposed to the energy rate payer) in line with other defence and security costs. This approach places the coverage of the costs beyond economic incentives.

The socio-economic costs of major power supply interruptions from accidental and malicious attacks are very high.[11] Given the heightened expectation of security risk to the energy networks, there is broad agreement among the sector regulators and decision makers that the security of these networks is a high priority and needs to be maintained.

In the event of major supply disruptions, economic regulation can also help alleviate the effect of supply shortages and minimise the economic and welfare effect of these. Competitive wholesale and retail energy markets balance the short-term demand and the available supply through the price mechanism.[12] However, contingency plans are needed for burden sharing in the event of medium-long term supply interruptions. The rational approach to burden sharing is to base these on social welfare and economic cost considerations.

The decision makers and regulators need to obtain estimates and decide on the appropriate level of investment on network security expenditures. These can be inferred from modelling the potential economic and welfare costs of low-probability high-

[10] Jamasb, T. and Nepal, R. (2014), Incentive Regulation and Utility Benchmarking for Electricity Network Security, Cambridge Working Papers in Economics 1434 / Energy Policy Research Group Working Paper 1413, Faculty of Economics, University of Cambridge.

[11] Nepal, R. and Jamasb, T. (2013), 'Security of the European Electricity Systems: Conceptualizing the Assessment Criteria and Core Indicators', *International Journal of Critical Infrastructure Protection*. 6(3-4), December, 182-196.

[12] Jamasb, T. and Pollitt, M. (2008), 'Security of Supply and Regulation of Energy Networks, *Energy Policy'*, 36(12), December, 4584-4589.

impact incidents.[13] The social welfare on households can be obtained from survey based contingent valuation methods.[14] For industrial and commercial users, this valuation can be based on modelling the cost of major interruptions to economic output taking into account the interdependencies among the different groups of users. It should be noted that the impacts of supply interruptions on individual industries can vary considerably in terms of their physical inoperability as opposed to economic cost due to loss of the output.[15]

Conclusions

Security of energy supply and infrastructure is a policy priority for most energy policymakers and regulators in both the EU and the USA. A sound regulatory approach with regards to network security needs to provide sufficient incentives to improve security to prevent outages but also to allocate and manage the supply shortfall in the event of major supply failures. However, the regulation of network security can also be understood in its wider economic regulation and national policy context. The harmonization of network security objectives and intensifying coordination among countries will be essential to deliver adequate supply security given its national importance and increasing international interdependencies.

---

[13] See the following: Poudineh, R. and Jamasb, T. (2015), Electricity Supply Interruptions: Sectoral Interdependencies and the Cost of Energy Not Served, OIES Paper: EL 12, Oxford Institute for Energy Studies, University of Oxford; Pindyck, R.S. and Wang, N. (2013), 'The Economic and Policy Consequences of Catastrophes' *American Economic Journal: Economic Policy,* 5(4): 306–339; and Nooij, M., Koopmans, C., and Bijvoet, C. (2007), 'The Value of Supply Security: The Costs of Power Interruptions: Economic Input for Damage Reduction and Investment in Networks', *Energy Economics,* 29: 277–295.

[14] See: Yu, W., Jamasb, T., and Pollitt, M. (2009), 'Willingness-to-Pay for Quality of Service: An Application to Efficiency Analysis of the UK Electricity Distribution Utilities', *The Energy Journal,* 30(4): 1-48 and Ofgem (2008), Expectations of DNOs and Willingness to Pay for Improvements in Service, Report prepared for Ofgem by Accent, Final Report, July, Office of Gas and Electricity Markets, London.

[15] See specifically the following: Poudineh, R. and Jamasb, T. (2015), Electricity Supply Interruptions: Sectoral Interdependencies and the Cost of Energy Not Served, OIES Paper: EL 12, Oxford Institute for Energy Studies, University of Oxford.